U.S. Department of Agriculture

Office of Inspector General
Financial & IT Operations

Audit Report

Natural Resources Conservation Service Application Controls – Program Contracts System (ProTracts)

Report No. 10501-5-FM
July 2006

USDA

UNITED STATES DEPARTMENT OF AGRICULTURE

OFFICE OF INSPECTOR GENERAL

Washington DC 20250

OFFICE OF INSPECTOR GENERAL OIG USDA

JUL 24 2006

REPLY TO
ATTN OF: 10501-5-FM

TO: Bruce Knight
Chief
Natural Resources Conservation Service

ATTN: Dan Runnels
Director of Operations Management and Oversight Division
Natural Resources Conservation Service

FROM: Robert W. Young Tracy LaPoint
for Assistant Regional Inspector General
for Audit

SUBJECT: Natural Resources Conservation Service
Application Controls – Program Contracts System (ProTracts)

This report presents the results of our audit of application controls in the Natural Resources Conservation Service's (NRCS) Program Contracts System (ProTracts). The report identifies additional policies, procedures, and system changes needed to ensure the confidentiality, integrity, and availability of data entered and stored in ProTracts. NRCS has reportedly taken significant actions to address the weaknesses we identified.

Your response to our draft report is included in its entirety in exhibit B, with excerpts incorporated in the Findings and Recommendations section of the report. Based on the information provided in the response, we have reached management decision for all recommendations except Recommendation 9. For Recommendation 9, additional actions are needed to reach management decision. Please refer to the OIG Position section of the report for specific details. Please follow your internal procedures in forwarding documentation of final action to the Office of the Chief Financial Officer for all other recommendations.

In accordance with Departmental Regulation 1720-1, please furnish a reply within 60 days describing the corrective actions taken or planned and the timeframes for implementation of the outstanding recommendation noted above. Please note that the regulation requires management decision to be reached on all findings and recommendations within a maximum of 6 months from report issuance.

We appreciate the courtesies and cooperation extended to us during the audit.

Executive Summary

Natural Resources Conservation Service Application Controls – Program Contracts System (Audit Report No. 10501-5-FM)

Results in Brief

The Natural Resources Conservation Service (NRCS) relied on the Program Contracts System (ProTracts) to manage its applications, contracts, and payment requests for four of its Farm Bill programs, which represented approximately $1.1 billion in outlays and obligations annually. The ProTracts system supports the critical component of NRCS' mission to provide leadership in a partnership effort to help farmers conserve, maintain, and improve the nation's natural resources and environment. Our objectives were to evaluate whether NRCS had adequate and effective controls over the input, processing, and output of ProTracts data.

Overall, we found that NRCS had not implemented adequate controls to ensure the integrity of NRCS data. As a result, NRCS cannot be assured that ProTracts data is complete, accurate, and reliable. Therefore, NRCS staff and management may not have the information they need to effectively manage its four Farm Bill programs.

The following summarizes the weaknesses the Office of Inspector General (OIG) identified.

- NRCS had not established program ownership of the ProTracts system or data. While NRCS relied on its technical group and a council of division managers, it did not recognize the importance of program management ownership. As a result, NRCS has reduced assurance that the ProTracts system and its other program-related systems meet the necessary internal controls required for its various Farm Bill programs to ensure effective and efficient program management.

- NRCS grouped the ProTracts system, along with numerous other major applications on multiple platforms, under its Conservation Program Delivery (CPD) group for system certification and accreditation (C&A) purposes. NRCS informed us that the systems in that group were integrated and intended to act as one cohesive system. However, in doing this, NRCS has reduced assurance that the necessary security controls are in place and functioning in ProTracts as intended.

- During another OIG audit, numerous weaknesses in the general support system environment that could adversely affect the reliability of ProTracts were reported.[1] The general support system is managed by a division of the Department's Chief Information Office, giving little oversight authority to NRCS. Without adequate controls within the general support system, the controls built into the ProTracts system could be rendered ineffective. For example, inadequate physical and environmental controls could render the system inoperable.

- NRCS did not ensure that only authorized users had permissions to ProTracts. NRCS did not have an effective process in place to manage its user accounts or access to its web services. Without these procedures operating effectively, NRCS was not able to ensure that its data was secure from unauthorized access or changes.

- NRCS could not ensure that changes to ProTracts were authorized, properly tested, and implemented. A well documented control process should at least include change request tracking, controlling source code, testing, and implementing system changes, as well as separating duties. NRCS' Information Technology Center (ITC) did not have policies, procedures, or controls in place to ensure that all the steps of a change control process were followed. Until an effective change control process is implemented, NRCS cannot rely on the integrity of the system.

- NRCS had not obtained security clearances for employees and contractors that are developing, maintaining, and using ProTracts. NRCS had not enforced the requirement that prerequisite clearances be obtained. Without these clearances, NRCS had reduced assurance that persons developing, managing, and using the ProTracts application and data could ensure its protection.

- NRCS had not implemented adequate controls to ensure that only authorized and complete data was entered and maintained in ProTracts. NRCS did not have established policies and procedures for reviewing and authorizing transactions. Field supervisors were responsible as contracting officers to authorize program contracts and thereby obligate funds and approve payments. We found that field supervisors differed in how and to what extent they reviewed transactions entered by their staff. As a result, NRCS had reduced assurance that complete and accurate data was entered and maintained in ProTracts.

[1] Audit Report No. 50501-3-FM, "Office of the Chief Information Officer – Management and Security Over Information Technology Convergence – Common Computing Environment," dated October 2005.

- ProTracts system controls did not always yield accurate payment information because of inconsistencies in unit values. NRCS officials stated that payments are computed based on verbal instructions provided by Headquarters staff. For the field staff to derive a payment, they had to manually calculate the payment and "plug" data into the system to arrive at the same result. This manual intervention, in an otherwise electronic process, increased the risk of improper payments.

Recommendations In Brief

We recommend that NRCS should:

- Assign program managers as system and information owners for its business critical applications, and establish definite roles and responsibilities between the program managers, the council, and the technical group.
- Reevaluate the accreditation decision and the documentation prepared during its C&A of the CPD group. Ensure that the accreditation is supported by complete, accurate, and trustworthy documentation which meets the requirements of NIST and Departmental guidance.
- Establish and implement policies and controls to ensure that employees and contractors are granted access to ProTracts using the concept of least privilege.
- Require NRCS to develop, document, and implement a complete change control process, including version control and testing, and establish controls to ensure the process is consistently applied.
- Establish controls to ensure that NRCS obtains and continually updates as required, the appropriate security clearances for all employees and contractors within NRCS and other agencies that are accessing ProTracts' sensitive data.
- Establish a policy and controls to ensure consistent performance of supervisory reviews for information entered into the ProTracts system.
- Establish automated controls within ProTracts to ensure payments are calculated accurately.

We made recommendations to correct general support system weaknesses in Audit Report No. 50501-3-FM, "Office of the Chief Information Officer – Management and Security Over Information Technology Convergence –

Common Computing Environment," dated October 2005. Therefore, we are making no additional recommendations in this report.

Agency Response

NRCS generally agreed with the findings and recommendations in this report. Its response is presented in its entirety as exhibit B.

OIG Position

We were able to reach management decision on all recommendations except Recommendation 9. Our position on what is needed to reach management decision on Recommendation 9 is outlined in the Findings and Recommendations section of the report.

Abbreviations Used in This Report

AMA	Agricultural Management Assistance
C&A	Certification and Accreditation
CCE	Common Computing Environment
CPD	Conservation Program Delivery
DM	Departmental Manual
eAuth	eAuthentication
EQIP	Environmental Quality Incentives Program
FSA	Farm Service Agency
GAO	U.S. Government Accountability Office
iCAMS	HR system
ID	Identification
ISSPOC	Information System Security Points of Contact
ITC	Information Technology Center, an operational support center of NRCS
ITS	Information Technology Service, a Division of OCIO
MOU	Memorandum of Understanding
NIST	National Institute of Standards and Technology
NRCS	Natural Resources Conservation Service
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
ProTracts	Program Contracts System
SCA	Service Center Agency
SDLC	System Development Life Cycle
SLA	Service Level Agreement
SP	Special Publication
USDA	U. S. Department of Agriculture
WHIP	Wildlife Habitat Incentive Program

Table of Contents

Executive Summary i

Abbreviations Used in This Report v

Background and Objectives 1

Findings and Recommendations 3

Section 1. Management of ProTracts Needs To Be Strengthened 3

Finding 1 Ineffective Organizational Structure 3
Recommendation 1 5
Finding 2 NRCS' Defined ProTracts Accreditation Boundaries Too Broadly 5
Recommendation 2 7
Finding 3 Weaknesses in the General Support System Environment Could Adversely Impact the Operations of ProTracts 8

Section 2. Ineffective Management of General Controls and System Vulnerabilities 10

Finding 4 Access Controls Are Inadequate 10
Recommendation 3 14
Recommendation 4 15
Recommendation 5 15
Recommendation 6 16
Recommendation 7 17
Finding 5 NRCS' Change Control Process Is Inadequate 17
Recommendation 8 19
Finding 6 Employees and Contractors With Significant System Responsibilities Did Not Have Appropriate Background Checks or Security Clearances 20
Recommendation 9 21

Section 3. Application Controls Need Strengthening 22

Finding 7 Controls Lacking for Review and Authorization of Transactions 22
Recommendation 10 23
Finding 8 Some ProTracts Payments Require Manual Intervention 23
Recommendation 11 25
Recommendation 12 25
Recommendation 13 25

Scope and Methodology 27

Exhibit A – ProTracts Application Controls Matrix 28
Exhibit B – Agency Response 30

Background and Objectives

Background

The Natural Resources Conservation Service (NRCS) is an agency in the U.S. Department of Agriculture (USDA) responsible for providing leadership in a partnership effort to help customers conserve, maintain, and improve the nation's natural resources and environment. With the 2002 Farm Bill legislation, Congress transferred the administrative responsibility for some of the Farm Bill programs from the Farm Service Agency (FSA) to NRCS. [2] The two agencies worked together to develop a migration plan for transferring the administrative responsibility, which was completed at the end of fiscal year 2003.

In order to assume this responsibility, NRCS developed and implemented the Program Contracts System (ProTracts), a web-based software system designed by NRCS to streamline the application and contracting process. NRCS' Information Technology Center (ITC) worked with national, State, and field staff to develop the system. It was implemented in phases, first with applications and contract tracking, and then the addition of payment requests through the Fund Manager interface. Currently, ProTracts is processing approximately $1.1 billion in obligations and payments for the four conservation programs using the system.

ProTracts is used to manage the conservation cost share and incentive contracts. Program participants may complete and submit program contract applications via the Internet. National and State program managers use ProTracts to allocate and track funds to States, counties, and special emphasis areas. ProTracts enables NRCS State office employees and field conservationists to create and manage contracts, certify completed practices, and request contract payments.

[2] Beginning in fiscal year 2004, ProTracts tracked applications and contracts for the Environmental Quality Incentives Program (EQIP), the Wildlife Habitat Incentives Program (WHIP), and the Agricultural Management Assistance (AMA) program. During the summer of 2004, WHIP and AMA payment requests were added to ProTracts. In addition, the Conservation Security Program applications, contracts, and payment requests were added in the fall 2004.
Payment requests for the largest Farm Bill program, EQIP, were added at the beginning of fiscal year 2005.

Payment requests are initiated in ProTracts and fed to the Department's Foundation Financial Information System for processing payments and preparing NRCS and Departmental financial statements.

Web and database servers for the ProTracts system are situated at the ITC, located in Fort Collins, Colorado. ProTracts uses USDA eAuthentication (eAuth) for initial access, with permissions further controlled by the system.

Application controls help make certain that transactions are valid, properly authorized, and completely and accurately processed by the computer. They are commonly categorized into three phases of a processing cycle.

- Input—data are authorized, converted to an automated form, and entered into the system in an accurate, complete, and timely manner.
- Processing—data are properly processed by the computer and files are updated correctly.
- Output—files and reports generated by the system actually occur and accurately reflect the results of processing and reports are controlled and distributed to the authorized users.

In addition, general security controls and automated controls built into the operating system that support the system should also be considered. Weak controls that allow physical or logical access to the computers that store system data could be used to circumvent the controls established within the system itself.

Objectives

Our objective was to determine whether NRCS had established adequate controls to ensure that data entered into ProTracts was properly authorized and completely and accurately processed.

Findings and Recommendations

Section 1. Management of ProTracts Needs To Be Strengthened

Management is responsible for developing and maintaining effective internal controls. The three objectives of internal control are to ensure the effectiveness and efficiency of operations, reliability of financial reporting, and compliance with applicable laws and regulations. Appropriate internal control should be integrated into each system established by agency management to direct and guide its operations.[3] While NRCS had implemented some controls within its ProTracts system, NRCS did not establish an effective security management structure including functional ownership, had not established certification and accreditation (C&A) boundaries that ensured adequate controls had been established over the ProTracts system, and did not adequately manage the general support environment in which ProTracts operates. Such conditions may lead to insufficient protection of sensitive or critical resources leaving the agency vulnerable to an attack by malicious users; thereby jeopardizing NRCS' ability to accomplish its mission.

Finding 1 Ineffective Organizational Structure

NRCS did not have a sufficient organizational structure in place to effectively manage the ProTracts application. NRCS management had not recognized the importance of assigning ownership of the ProTracts application to an individual or group responsible for ensuring the application met the intent of the agency's mission in delivering its programs. Individuals with information technology (IT) responsibilities and knowledge are not necessarily in a position to ensure the agency's mission responsibilities are given the appropriate priority. This ultimately may affect NRCS' ability to adequately manage its efforts to conserve, maintain and improve the Nation's natural resources for the four affected Farm Bill programs serviced by ProTracts. NRCS indicated that it had started taking action to address issues identified during the audit regarding ProTracts management prior to the issuance of this report.

[3] The Office of Management and Budget (OMB) Circular No. A-123, "Management's Responsibility for Internal Control," dated December 21, 2004.

OMB states that appropriate internal control should be integrated into each system established by agency management to direct and guide its operations. Internal control applies to program, operational, and administrative areas as well as accounting and financial management. The National Institute of Standards and Technology (NIST) provides that the responsibility for establishing the controls for information generation, collection, processing, dissemination, and disposal rests with the information owner, who is an agency official with operational authority for the specified information.

System Development Life Cycle (SDLC) requires that at least two groups should be in place: (1) a project management committee and (2) a functional program and administrative management group. The project management committee should perform functions such as mediating priorities relating to business area analysis, software development, system deployments, training, and maintenance. The functional management group, on the other hand, should maintain a list of proposed enhancements from staff throughout the organization, develop functional and technical requirements for these items, and provide operational support on a day-to-day basis.

NRCS entrusted system ownership of ProTracts, as well as its other systems, to its ITC group, and established a business council of key agency leaders to ensure that all elements of system requirements are integrated and implemented in a timely manner. However, NRCS did not assign a program official knowledgeable in routine system operations. Without this involvement, ITC could not ensure that both the program and technical related system requirements are met. Not involving a knowledgeable program official in the process resulted in a significant lack of separation of duties. For example, ITC is currently maintaining a list of enhancements from staff throughout the organization, developing functional and technical requirements for these items, and prioritizing the requests, as well as providing operational support. Knowledgeable program officials should be designated as the system and information owners to develop the functional requirements of system enhancements, ensure the most critical enhancements are made timely, and be involved in system testing to ensure the accuracy and completeness of the system changes. This level of involvement ensures that program-related internal controls are met.

Recommendation 1

NRCS should assign program managers as system and information owners for its business critical applications and establish definite roles and responsibilities between the program managers and the technical group.

Agency Response

NRCS formed and staffed an agency field business tools team within the Programs Deputy area to provide business ownership and direct guidance to the core agency program delivery applications, including ProTracts, and associated support applications. The Deputy Chief for Programs was assigned ownership for the ProTracts system. Two program business experts also were assigned to the Fort Collins, Colorado location to provide day-to-day guidance to the ITC responsible for maintaining and enhancing the core applications. This has enabled the ITC to focus on its IT technical responsibilities.

In addition, NRCS will complete an update to its entire automated business tools policy documentation by September 30, 2006, which will include the definition, roles, and responsibilities of the revised management structure around the core business applications.

OIG Position

We concur with NRCS' management decision on this recommendation.

Finding 2 NRCS' Defined ProTracts Accreditation Boundaries Too Broadly

NRCS grouped the ProTracts system, along with numerous other major applications, under its Conservation Program Delivery (CPD) group for system C&A purposes. NRCS informed us that the systems in that group were integrated and intended to act as one cohesive system. However, in doing this, NRCS has reduced assurance that the necessary security controls are in place and functioning in each application as intended.

NIST provides guidelines for systems supporting the executive agencies of the Federal Government. [4] NIST considers the C&A process to be an important activity that supports risk management and should be an integral part of an agency's information security program. NIST guidelines have been developed to assist Federal agencies to achieve more secure information systems. Establishing adequate accreditation boundaries has significant security implications, including consideration of the mission/business requirements of the agency, the technical considerations with respect to information security, and the programmatic costs to the agency. Accreditation boundaries that are unnecessarily expansive (i.e., including too many hardware, software, and firmware components) make the security C&A process extremely unwieldy and complex. Agencies need to establish their boundaries before they conduct the initial risk assessments and develop system security plans since the scope of these documents rely on the accreditation boundaries.

NRCS' CPD group contained seven systems involving more than 50 business applications that support its core mission. These applications were in mixed stages of SDLC and used different technologies, including mixed program specific applications along side administrative applications (i.e., time and attendance). By grouping these varied applications, NRCS does not have sufficient management and planning in place for its major applications, which should be considered subsystems of the CPD group. By accrediting a system or subsystem, NRCS does not devote sufficient planning and oversight to its major applications. Further, the NRCS accreditation official cannot make an informed decision about acknowledgment and acceptance of system-specific weaknesses and risks.

In addition to the broad system boundaries, we found that NRCS had not completed disaster recovery and configuration management plans for the CPD group of systems. These documents are critical to the accreditation decision in determining whether adequate controls are in place to accept system risk. Despite the broad system boundaries and missing documentation, NRCS still accredited the CPD group of systems as a whole without limitations.

[4] NIST Special Publication (SP) 800-37, "Guide for the Security Certification and Accreditation of Federal Information Systems," dated May 2004. For the accreditation boundaries, see Section 2.3.

Recommendation 2

Reevaluate the accreditation decision and the documentation prepared during its C&A of the CPD group. Ensure that the accreditation is supported by complete, accurate, and trustworthy documentation which meets the requirements of NIST and Departmental guidance.

Agency Response

NRCS defined 20 security C&A subsystem boundaries within the three primary agency IT investments. A specific C&A subsystem boundary was established for ProTracts within the CPD investment. The 20 new subsystems were vetted with USDA Cybersecurity in December 2005, which approved and gave the "green light" to proceed.

A C&A was performed on the ProTracts subsystem during the period of August through November 2005. After some difficulty engaging a Department acquisition vehicle, a Security Testing and Evaluation (ST&E) is currently underway by an independent contractor, and is expected to be completed by the end of June 2006. As required, the three investment-level systems, including CPD, and the 20 subsystems, including ProTracts, have been put on a 3-year recertification rotation.

OIG Position

We concur with NRCS' management decision on this recommendation.

Finding 3

Weaknesses in the General Support System Environment Could Adversely Impact the Operations of ProTracts

We identified numerous weaknesses in the general support system environment that could adversely affect the reliability of ProTracts. The general support system is managed by a division of the Department's Office of the Chief Information Officer (OCIO), giving little oversight authority to NRCS. Without adequate controls within the general support system, the controls built into the ProTracts system could be rendered ineffective.

Information Technology Services (ITS), a division of OCIO, has the responsibility for maintaining the network infrastructure and hardware on which the ProTracts system resides. We recently completed a review of the common computing environment (CCE).[5] Since NRCS is one of the service center agencies (SCA) supported by ITS, the weaknesses identified in that audit have a direct effect on ProTracts. Until the issues are resolved within CCE, additional oversight or controls need to be established to ensure the accuracy and reliability of ProTracts data.

The following are, in our view, the most significant issues from that report which affect ProTracts.

- The Department had not finalized operating procedures. Instead, field support personnel were relying on SCA operating procedures in place prior to convergence to CCE. Further, ITS had not established a formal procedure for drafting, commenting, or finalizing operation procedures and other policy documents.

- The Department implemented a memorandum of understanding (MOU) and Incidental Transfer Agreement that were too overarching to hold either ITS or its SCAs accountable for adequate security. Further, only two of the three agency representatives had signed the final MOU. As

[5] OIG Audit Report No. 50501-3-FM, "Office of the Chief Information Officer Management and Security Over Information Technology Convergence – Common Computing Environment," dated October 2005.

a result, clear lines of authority or accountability had not been established for carrying out security effectively.

- The Department had not begun periodic scanning of the CCE network and SCAs had ceased their scanning activities after CCE convergence in November 2004. The review disclosed that (1) a large number of risk indicators that may be exploitable, including risk indicators on the ProTracts servers, and (2) system policy settings did not provide for optimum security and were not uniform throughout the CCE network. Therefore, the CCE systems and networks may be vulnerable to cyber-related attacks, jeopardizing the integrity and confidentiality of SCA systems and data.

- Physical and environmental controls needed improvement. We visited one of the three Web Farms, three State offices, and 19 service centers and found inadequate physical and environmental controls over computer equipment. At the State offices and service centers, we found that the server cabinets were being used for storage, not fully assembled, and located near water sources. At the Web Farm, which ProTracts resides on, the team found that access to the server room was not limited to only those individuals with a need for access and that the air conditioning units were unable to cool the room adequately, resulting in several servers needing to be shut down. As a result, ITS and the agencies it serves have reduced assurance that computer resources are adequately protected from physical and environmental vulnerabilities.

We are not making any specific recommendations within this report. We made recommendations addressed to OCIO-ITS in Audit Report No. 50501-3-FM to resolve these issues.

Section 2. Ineffective Management of General Controls and System Vulnerabilities

General controls are the structure, policies, and procedures that apply to an entity's overall computer operations. They create the environment in which application systems and other controls operate. General controls include access controls, application software development and change controls, and segregation of duties.[6] We found that NRCS did not have effective controls in place to ensure that (1) access to ProTracts was controlled, (2) a structured change control process was followed, (3) background checks and security clearances had been completed, and (4) user training was completed. Without effective general controls, application controls may be rendered ineffective by circumvention or modification.

Finding 4 Access Controls Are Inadequate

NRCS did not ensure that only authorized users had permission to ProTracts data. USDA eAuth and system permissions, as well as web services, were used to access the data. NRCS did not have an effective process in place to manage user accounts or access to web services. During our review, NRCS recognized these access problems and began to develop some basic process information. However, without these procedures operating effectively, NRCS was not able to ensure that its data was secure from unauthorized access or changes.

OMB requires the use of individual accountability, least privilege, and separation of duties controls in every application.[7] In addition, Departmental regulations require security staff to maintain files of users, including names, office addresses, and telephone numbers. Additionally, user identifications (ID) and passwords can be assigned only to authorized individuals; no generic or shared user IDs are to be created. Finally, security staff need to remove user accounts when the employee is no longer with the agency. To ensure

[6] The U.S. Government Accountability Office (GAO) "Federal Information System Controls Audit Manual," dated January 1999.

[7] OMB Circular No. A-130, "Security of Federal Automated Information Resources," via Transmission #4, dated November 28, 2000.

removal, formal procedures should be established for agency personnel to notify security staff of all separations.[8]

We identified weaknesses in several areas related to access to ProTracts. The following sections describe the weaknesses we identified.

eAuth Access

NRCS used the Department's eAuth system to enable customers, affiliates, and employees to access USDA web software and services via the Internet. Instead of removing security assignments within the system when users became separated, NRCS relied on the Department to deactivate the user's eAuth account. We identified the following issues with eAuth.

- Active eAuth accounts for NRCS employees and contractors that were no longer employed by NRCS were identified. NRCS staff informed us that the NRCS human resources group did not keep its human resources system current which contributed to eAuth not being updated. We noted 13 active eAuth accounts for former employees.

- A user logging into eAuth established a 9 hour active session. If the user became inactive for approximately 1 hour, then their session was terminated. The ProTracts system provided for 1/2 hour of inactivity before a user is logged out of ProTracts. However, unless the user exited the Internet browser entirely, the user was able to enter ProTracts without being prompted for a login and password. ProTracts inactivation times were superceded by those established for eAuth and may not allow the system to be as secure as intended.

- NRCS had not executed a Service Level Agreement (SLA) with OCIO for their eAuth security interconnection. A formal SLA should be in place to document each group's

[8] Departmental Manual (DM) 3140-001, "Management ADP Security Manual," dated July 19, 1984.

understanding of the interconnectivity between systems, including ProTracts, iCAMS, and eAuth.[9]

During the course of our audit, NRCS officials began to develop forms and flowcharts to describe the process to update eAuth security roles more timely. Until these procedures are fully implemented, NRCS cannot be assured that its data is secure from unauthorized access or changes.

ProTracts Permissions

"Super User" permissions were granted to system support staff to administer the system and assist in troubleshooting user problems. This level of access, provided to four NRCS employees and nine contractors, allowed the support staff to impersonate a system user such that the support staff saw exactly what the user was experiencing. This allowed the support staff to assist the user through the issue or identify a technical issue that required a change to the system. While this level of access may assist in resolving user issues, it also allows those with this privilege the ability to bypass system controls. We identified the following weaknesses with this Super User privilege.

- Instead of using an automated routine, the security for this role was "hard-coded" into the login screen for the system. For example, the system administrator had to request a manual change in the programming to activate or deactivate Super User permissions.

- The system support staff was able to make changes to production data under any user's ID. The information appeared to have been performed by the individual being impersonated.

- Of the nine contractors with the Super User permissions, we identified two were no longer under contract with NRCS. The first contractor left in February 2004 but did not have an active eAuth account. The second contractor left in January 2005 and still had an active eAuth account.

[9] OMB Circular No. A-130, Section 8, requires agreements between service recipients and service providers. Appendix III further details the agreements for system interconnection and information sharing. In addition, NIST SP 800-47, "Security Guide for Interconnecting Information Technology Systems," provides in the Executive Summary that it contains guides and samples for developing an Interconnection Security Agreement and a MOU/Agreement, which are forms of SLAs.

This meant the second contractor could continue to access the ProTracts system as a Super User from within the USDA infrastructure.

- Of the 11 remaining Super Users, 5 of them were no longer working with ProTracts and therefore, should not require this level of access.

ProTracts also had user privileges for each State. Individual State administrators assigned these permissions to individuals based on counties or State level access needs. We identified several weaknesses with these user permissions.

- More than 120 system users had in excess of 150 security assignments within the system. A security assignment was defined by program, role, and location (e.g., county, State). This number of security roles made it difficult to manage and validate what data the user could access or change.

- At least two user IDs were generic accounts. User accounts should be specific to individual users as to ensure the ability to determine who made changes to system data.

Web-based Access

NRCS cannot ensure that only authorized users have access to Privacy Act protected data. We were able to obtain information containing sensitive producer information for farm program eligibility. NRCS and FSA, who managed the website, did not have an effective technical solution in place to manage access to this and other sites. NRCS and FSA officials recognized the problem and informed us that they were working to identify a long-term solution for all web sites with this issue. However, until stronger controls are established, the agencies cannot prevent unauthorized access to sensitive data.

Other Access Issues

We found a number of other inadequate access control issues.

- NRCS employees and contractors, who performed database development, had access to the production databases. ITC acknowledges that these individuals made changes to the production databases as needed, however, it is a common separation of duties practice to deny database developers access to production databases. In addition, we found that production database changes were not tracked. (See Finding No. 5.)

- Many individual screensavers were set to allow significant time to pass before the computer was locked due to inactivity. At four of the six counties we visited users set screensavers to lock their computers after more than 30 minutes. We found one user that set his screensaver to 1,000 minutes.

- Generic accounts were used on workstations at one State office we visited. The staff had no idea who had passwords or who used the accounts. Additionally, the support staff had not deleted the accounts because of directions from Headquarters staff.

Recommendation 3

NRCS should coordinate with eAuth staff to develop and implement reliable policies and controls to ensure that eAuth accounts that have access to NRCS systems are kept current.

Agency Response NRCS will complete a SLA with eAuth by July 31, 2006.

NRCS human resources (HR) specialists update the Human Resources Information System (HRIS), formerly the iCAMS and in the future to be EmpowHR, when an employee is terminated. The change is electronically updated in the National Finance Center (NFC) employee database, from which a BEAR file is created, which eAuth reads and the account is deactivated.

The primary access control for NRCS partner employees (affliates) is a monthly information system security points of contact (ISSPOC) review and reconciliation of CCE accounts. The CCE account is central to whether an affiliate can access ProTracts and other agency core applications. An affiliate with a terminated CCE account may still retain their eAuth account for other purposes with USDA.

The Department has been reticent to integrate CCE and eAuth accounts, saying that Homeland Security Presidential Directive-12 would resolve the matter. In the meantime, NRCS intends to automate the management of CCE account relationships with affiliates, eAuth and iCAMS to make it easier for ISSPOCs to perform their duties. The automated process is expected to be completed and deployed by December 31, 2006.

Recommendation 4

NRCS should establish policies and controls to ensure that ProTracts accounts used by separated employees are timely removed.

Agency Response

ProTracts users must have a CCE account and an eAuth account to run the application. NRCS revised and strengthened its access control process in July 2005 by establishing ISSPOCs in each State, region, and national organizational unit to keep CCE accounts current. Written procedures were provided to all ISSPOCs with appropriate training. ISSPOCs are required to update agency, partner, and contractor CCE accounts on a monthly basis. CCE account data feeds are provided to ISSPOCs on a monthly basis to assist in removing accounts for terminated employees, duplicate accounts, and non-cómpliant group or generic accounts.

NRCS is building a new core business application authorization service, which ProTracts will use starting October 1, 2006. The new service will contain improved procedures and guidance for timely management of ProTracts user permissions, including removal when an employee is no longer authorized.

Recommendation 5

NRCS should establish and implement policies and controls to ensure that all employees and contractors are granted access to ProTracts using the concept of least privilege.

Agency Response

NRCS is building a new core business application authorization service which ProTracts will use starting October 1, 2006. The new service is designed on the concept of "least privilege," the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

In the meantime, super user access to ProTracts has been curtailed to essential active application maintenance staff, and guidance has been provided to State ProTracts administrators to apply "least privilege" principles to user permissions. The NRCS Information System Security Officer (ISSO) has been assigned to monitor ProTracts user permissions to advise the Chief Information Officer if additional steps are needed.

To reinforce segregation of duties, NRCS also intends to divide ITC into an Application Operations Branch and a Business Application Development Branch. The application maintenance function will be the responsibility of the operations branch. The Development Branch staff will not be permitted access to the production hosting environment, including the deployed application and databases. This modification to the organization is expected to be completed by December 31, 2006.

Recommendation 6

NRCS should establish controls to ensure that only authorized users can access sensitive information from its web-based applications.

Agency Response

NRCS has worked with the FSA to secure access to its Web services for customer data and producer eligibility. There are two phases: programmatic and hardware-dependent. The programmatic phase has been completed. Both NRCS and FSA are working with the Office of the Chief Information Officer (OCIO) ITS to utilize a hardware accelerator installed in the USDA hosting environment to further secure the use of Web services across applications and agencies. The latter phase is expected to be completed by September 30, 2006, although the date depends on resolution of the OCIO ITS operational and budget issues.

Recommendation 7

NRCS should determine a reasonable inactivity time and develop/implement code per that specification based on its risk assessment of ProTracts.

Agency Response

NRCS has established a 30-minute time-out for all core program delivery business applications. ProTracts users must re-authenticate through eAuth after a 30-minute inactivity period in the application.

OIG Position

We agree with NRCS' management decision on these recommendations.

Finding 5 NRCS' Change Control Process Is Inadequate

NRCS could not ensure that changes to ProTracts were authorized and properly tested and implemented. The change control process should (1) document change requests and authorizations, (2) safeguard source code, (3) document testing and the results, and (4) implement only approved system changes. ITC did not have policies, procedures, or controls in place to ensure that all the steps of a change control process were followed. Until an effective change control process is implemented, NRCS cannot rely on the integrity of the system.

The Department requires that all major application systems have a properly documented change control process. Such a process is used to maintain software integrity, minimize life cycle software costs, prevent unnecessary or marginal changes, establish change priorities, assure prompt action on changes, document the changes, and control the release of changed software and documentation. Based on this process, changes to systems should be grouped logically into version numbers and then analyzed, developed, and tested within this grouping. [10]

ITC acknowledged that this process needed to be further developed and implemented. ITC personnel stated they had begun developing a process to ensure that NRCS systems will be more consistently managed, however, they had not yet

[10] DM 3520-001, "Chapter 4, Part 1 – CM Policy and Responsibilities," dated July 15, 2004.

drafted the policies or procedures, nor were they able to provide a timeframe when the new process and standards would be implemented. In the meantime, NRCS cannot attest to the integrity of changes made to ProTracts.

We found that ITC had not documented its changes to ProTracts. A well documented control process should at least include change request tracking, controlling source code, testing, and implementing system changes, as well as separating duties. ITC did not have documentation for these items. For example, ITC had not documented how changes developed for the system are tested, including the environment to be used for testing or the tests to be performed and the results. In addition, ITC did not have any documentation for implementing system changes and relied on one contract staff person to implement changes.

We also found that ITC did not maintain adequate software version controls which would ensure that an audit trail of system changes was maintained and that changes could be rolled back if necessary. Multiple releases were performed within a single version number. ITC's process for software versioning prevented it from being able to rebuild anything but the most current version of the application's software. Without better versioning and with no audit trail of changes, ITC would not have the ability to recover the application if a disaster occurred or be able to revert to a prior version of the application if needed.

Finally, ITC did not have a documented testing process that consistently applied to its application changes, including test cases or scenarios for consistent regression testing with new application releases.[11] Testing is integral to ensuring that changes to a system are meeting the user's objectives. In a complete change control process, testing should include user approval to validate the purpose of the changes. Further, ITC had no controls in place to ensure that they consistently performed tests to ensure the system's security integrity is maintained.

[11] NIST Special Publication (SP) 800-18, "Guide for Developing Security Plans for Information Technology System," dated December 1998. See Section 6.MA.2 for guidance on Logical Access Controls.

Recommendation 8

ITC should develop, document, and implement a complete change control process, including version control and testing, and establish controls to ensure the process is consistently applied.

Agency Response NRCS has migrated all agency business applications, including ProTracts, to a common project management and system lifecycle tool called COLAB. This authenticated Web-based tool provides source code and executable version control, change management, and trackers for defects, features, and issues. The tool also includes system documentation, forums, and project team managements. Configuration management and change control policy has been updated. Integration testing and certification has been more cleanly segregated from development.

NRCS has established a project management office (PMO) function to monitor compliance across all development teams and projects with the standard system lifecycle process. Agency budget allocations to IT development projects require compliance and support services contract work authorization orders contain clauses requiring the use of COLAB.

COLAB and the PMO function will be institutionalized in the comprehensive NRCS IT policy update on September 30, 2006. The PMO function will be reflected in revised NRCS IT staffing plans, expected to be approved and in place by December 31, 2006.

OIG Position We agree with NRCS' management decision on this recommendation.

Finding 6 Employees and Contractors With Significant System Responsibilities Did Not Have Appropriate Background Checks or Security Clearances

NRCS had not obtained security clearances on employees and contractors that are developing, maintaining, and using ProTracts as required by Departmental standards. NRCS had not made this a priority within their human resources group. Without these clearances, NRCS had reduced assurance that persons developing, managing, and using the ProTracts application and data could ensure its protection.

The Department requires clearance of all persons involved in the development, management, and operation of sensitive systems and facilities. These requirements apply equally to Federal employees, contractors for the Federal Government, and nonFederal employees such as State and local government workers having access to sensitive Federal data. Appropriate agency authority will determine requisite clearance levels for positions in all cases.[12]

NRCS had a variety of individuals accessing the sensitive data stored within its ProTracts system, including:

- ITC employees and contractors, who developed and implemented the software systems;
- NRCS employees within the national, State, and local offices, who used the system; and
- nonFederal, State, and local employees and contractors, who accessed information.

In addition, NRCS was unable to provide documentation showing which individuals had security clearances or even basic background screenings. NRCS did not maintain records regarding this information.

[12] DM 3140-001, "Management ADP Security Manual," dated July 19, 1984.

Recommendation 9

NRCS should establish controls to ensure that NRCS obtains and continually updates as required, the appropriate security clearances for all employees and contractors within NRCS and other agencies that are accessing ProTracts' sensitive data.

Agency Response

In response to security C&A of the three primary NRCS IT investments and other oversight reviews and audits, the agency has taken steps to close the gap in background investigations (BIs) among employees, partners, and contractors working connected to the USDA network (having CCE accounts). All must have a suitable BI on file or in progress by September 30, 2006.

Since the ProTracts audit, the improved NRCS access control process requires that all new employees, partners, and contractors must have at least a suitable BI in progress in order to obtain their CCE account. Users cannot access ProTracts unless they have a CCE account.

OIG Position

We concur that NRCS' improved access control process is a positive step. However, to achieve management decision on this recommendation BIs need to be completed (not in progress) prior to granting an employee or contractor access to ProTracts.

Section 3. Application Controls Need Strengthening

Application controls help ensure that transactions are valid, properly authorized, and completely and accurately processed and reported. Application controls include (1) controls built into the application itself and (2) manual follow up of computer-processed and generated information. Application controls must be effective to help ensure the reliability, appropriate confidentiality, and availability of critical automated information.[13] We found that NRCS lacked controls to ensure (1) data entered into ProTracts was authorized and (2) payment calculations were accurate. Without these controls, NRCS was not able to ensure that transactions entered into the system were valid and properly authorized, and ProTracts completely and accurately processed and reported Farm Program data.

Finding 7

Controls Lacking for Review and Authorization of Transactions

NRCS had not implemented adequate controls to ensure that only authorized and complete data was entered and maintained in ProTracts. NRCS did not have established policies and procedures for reviewing and authorizing transactions. Field supervisors were responsible as contracting officers to authorize program contracts and thereby obligate funds and submit payment requests. We found that field supervisors differed in how and to what extent they reviewed transactions entered by their staff. As a result, NRCS had reduced assurance that complete and accurate data was entered and maintained in ProTracts.

GAO provides that policies and procedures should be developed to ensure that internal controls are an integral part of its operations.[14] For example, managers should be reviewing information entered into the system and reports generated by the system.

We asked NRCS field supervisors how and to what extent they reviewed transactions entered by their staff. One supervisor

[13] GAO's "Federal Information System Controls Audit Manual," dated January 1999.
[14] GAO's "Standards for Internal Controls in the Federal Government," on page 7, dated November 1999.

indicated that they review field notes and system generated applications, contracts and related modifications, and payment requests for approximately 90 percent of the contracts within their office. Another supervisor told us that they only reviewed data when their staff had a problem.

Recommendation 10

NRCS should establish a policy and controls to ensure that only authorized and complete data is entered in ProTracts.

Agency Response

Policy and guidance in "Conservation Program Contracting" (GM 440 part 512) was revised and issued to better document policy and procedures for reviewing and authorizing transactions associated with ProTracts contracts and payments. National training and Internet conferences were held to further ensure field, State, and national staff understanding of internal controls and their responsibilities.

Additional tools have been added to ProTracts/Fund Manager to assist supervisors and payments approvers in reviewing transactions. Internet conference training (recorded for later review by field and other staffs) included demonstration and guidance on use of numerous online reports to monitor and review contract transactions.

OIG Position

We agree with NRCS' management decision on this recommendation.

Finding 8

Some ProTracts Payments Require Manual Intervention

ProTracts system controls did not always yield accurate payment information because of inconsistencies in unit values. Contract and system payment calculations did not always use the same unit measurements to derive values. NRCS officials stated that payments are manually calculated based on verbal instructions provided by Headquarters staff. For the field staff to compute a payment, they had to manually calculate the payment and "plug" data into the system to arrive at the same result. This manual intervention, in an otherwise electronic process, increased the risk of improper payments.

GAO requires agencies to establish controls over its information to help ensure completeness, accuracy, authorization, and validity of all transactions during processing.[15]

NRCS field staff informed us that ProTracts had not calculated some payments as they would expect based on inherent knowledge of the contract. They indicated that the system was not rounding payments accurately, or using the same unit of measurement for the payment calculation as for the contract amount. For example, pipeline costs used in a project are calculated on diameter and linear feet. The payment calculation in ProTracts does not include diameter. In addition, we found that ProTracts had not limited total payments to the contract value for the individual contract items. Field staff indicated they often made manual adjustments to the completed units to derive the payment amount they expected.

Further, NRCS did not have documented procedures for how payments should be calculated within ProTracts. ITC indicated that they have worked with Headquarters staff to determine how the calculations should be made. In addition, national office staff indicated that they had directed field staff not to make changes to the units, as noted above, but to notify them when payments were incorrect. However, the field staff we spoke with showed us how their manual process ensured that the "correct" payment amounts were made. Finally, this manual process in an otherwise automated system introduced the risk of erroneous payments because of human error. Our tests validated the field staffs concerns with the ProTracts payment calculations; however we did not attempt to quantify the magnitude of these problems. We plan on testing payment calculations in our upcoming Improper Payment Act audit.

In addition, NRCS did not have policies or procedures for reconciling the appropriations, obligations, or payments between ProTracts and the Department's financial system after FSA balances were initially entered into ProTracts. Each NRCS group that we spoke with did not believe that this was their responsibility. Without this reconciliation, NRCS cannot

[15] GAO's "Standards for Internal Control in the Federal Government," dated November 1999.

ensure that the two systems are reporting the same appropriations, obligations, and payments.

Recommendation 11

NRCS should document its payment calculation process for all its payment scenarios.

Agency Response

NRCS completed documentation of the ProTracts system including all payment calculation scenarios. This documentation was approved by the ProTracts owner, checked into the COLAB repository, and placed under change control.

The NRCS payment calculation process is documented and a signed copy is stored in COLAB.

Recommendation 12

NRCS should establish automated controls within ProTracts to ensure payments are calculated in accordance with its payment process.

Agency Response

NRCS completed several automated control enhancements to ProTracts to ensure that payments are calculated in accordance with the NRCS payment process. Interface changes allow users to review payment calculations, tighter process controls better prevent users from overriding payment calculation rules, and new controls have been implemented to reduce chances of an erroneous payment.

In addition to automated controls, NRCS requires two people to review and approve payments. The first request for payment happens at field level and uses ProTracts. Payment calculation and documentation are then further reviewed and approved by the FFIS user. The double approval helps ensure only proper payments are made.

Additional documentation of procedures and training has been provided to better inform field staff of automated controls and how ProTracts calculates payments.

Recommendation 13

NRCS should establish effective policies and procedures to ensure that the ProTracts appropriations, obligations, and payments are reconciled to the amounts recorded in the Department's financial system on a timely basis.

Agency Response

NRCS has established effective controls and procedures to ensure ProTracts allocations (appropriations), obligations, and payments are reconciled on a timely basis. NRCS has established a nightly data feed from FFIS of current allocations, obligations, and payments. This information is updated in the ProTracts database to ensure current obligations cannot exceed allocations. Any differences in obligations and payments are flagged and identified in reports.

Additional reports have been added to ProTracts to facilitate daily, weekly, and monthly reconciliation activities. Training on policy and procedures in using these reports has been provided.

OIG Position

We agree with NRCS' management decision on these recommendations.

Scope and Methodology

We reviewed application controls over the ProTracts system established by NRCS to ensure the confidentiality, integrity, and availability of information in that system. The review was conducted at NRCS Headquarters in Washington, D.C., one State office, and six county offices. The State and county offices were judgmentally selected based on the program dollars and locations. In addition, our review was also conducted at the Fort Collins ITC facility where the web software was developed and production servers reside.

Fieldwork was performed from February through June 2005.

To accomplish our audit objectives, we performed the following audit steps and procedures.

- Reviewed policies, procedures, and system documentation when available relating to the ProTracts system;

- interviewed NRCS officials responsible for the development, management, and data input of the ProTracts system;

- interviewed NRCS State and field staff responsible for data authorization, completeness, and accuracy at selected State and county offices;

- analyzed user account information in regards to accessing ProTracts data; and

- briefly reviewed system source code and data records to verify the integrity of ProTracts data.

This audit was performed in accordance with "Government Auditing Standards."

Exhibit A – ProTracts Application Controls Matrix

Control Objective (Based on GAO Federal Information System Control Audit Manual)	ProTracts Control Technique(s)[16]	OIG Results
All data are authorized before entering the application system.	• Data are collected and analyzed by field staff. • Data are then entered by field staff into applications, contracts, contract status, and/or payment requests.	• The field staff that we talked to indicated that their notes and the information that they collect are placed in contract files. This information is then available to management for their review. • District conservationists did not seem to have a consistent review process in place for reviewing information entered into ProTracts. We also expect that review processes within the State offices will vary as to how it is completed.
Restrict data entry terminals to authorized users for authorized purposes.	• User IDs and passwords are required on field, district, and Headquarters computers. • User IDs and passwords are required to gain access to eAuth. Then a single sign-on process allows the user ID to enter the ProTracts and Fund Manager interfaces. • User IDs are limited access to ProTracts data based on assigned permissions. • Fund Manager access is based on having an eAuth account. • A Super User role is available for ProTracts which allows system support staff to impersonate users. • Password-protected screensavers locked access to computers. • Only specifically approved phone numbers are allowed to dial into the ProTracts web server, primarily for server support. • ProTracts limits the user to 1/2 hour of inactivity before the user must reenter the system. In addition, eAuth access is limited to 1 hour of inactivity or 9 hours of time.	• Field staff's computers were not always physically protected from unauthorized access. • ITC indicated that ProTracts maintains a log of activities performed by users. • NRCS does not have an executed interconnectivity agreement for eAuth. • Password age for eAuth accounts was not set in accordance with Departmental and NIST guidelines. • eAuth and ProTracts permissions were still active for inactive employees and contractors. • While the security model for ProTracts is very flexible, more than 120 users had more than 150 security accesses. • Fund Manager needs more security based on the least privilege concept. • Database developers have access to make changes to production databases. • Employees and contractors did not have prerequisite background checks and security clearances for the data being accessed. • Most of the screensavers we reviewed allowed too much time to pass before locking the computer. • Modem access to the server is limited to only approved phone numbers. • NRCS does not have clear definition regarding the amount of time that a user can be logged on inactively. eAuth access for up to 9 hours could allow someone access to ProTracts for longer than anticipated. • Security to Web Services interconnected to ProTracts is not as strong as it should be.

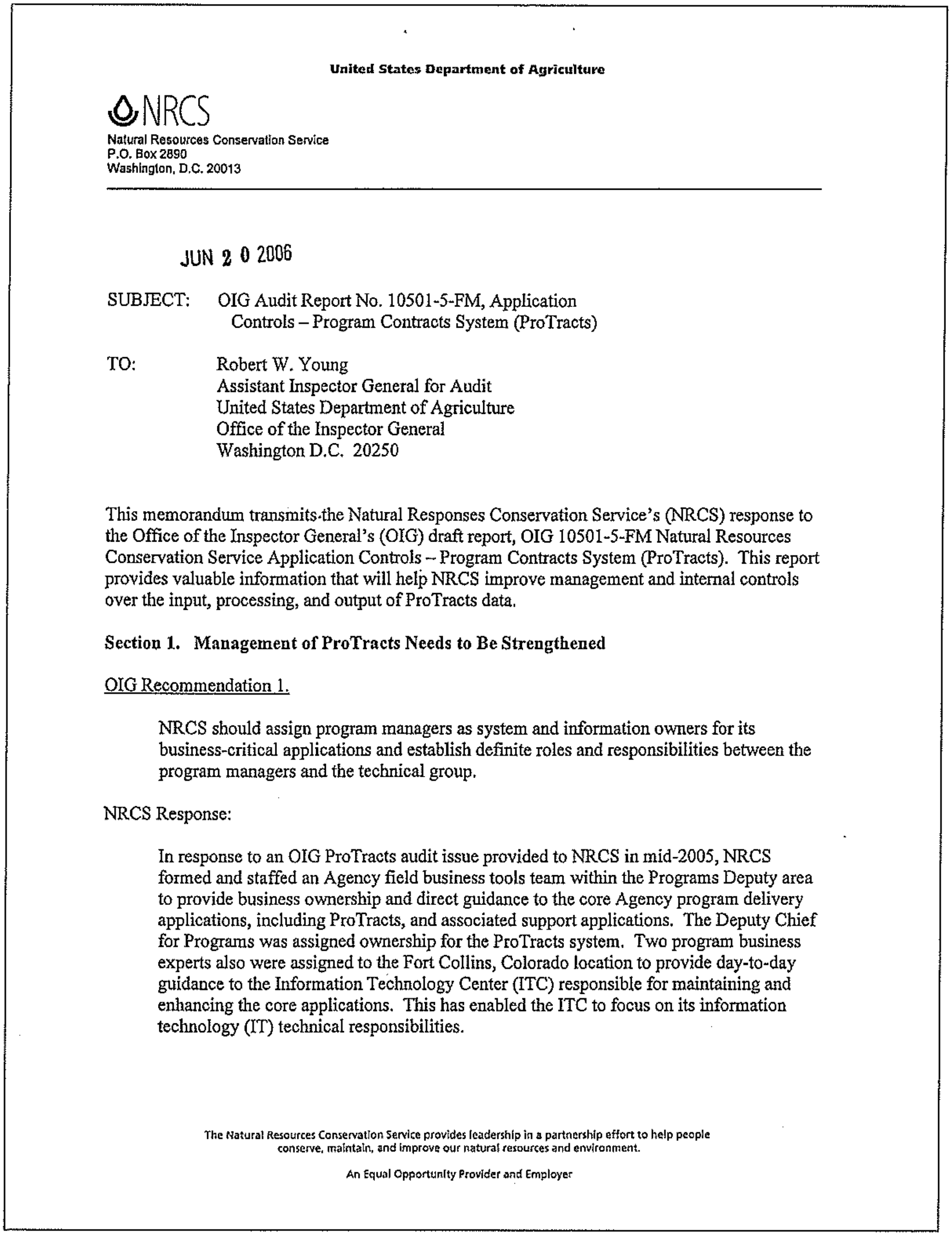
[16] ProTracts control techniques as reported to us by NRCS officials. Only limited system documentation existed outlining the controls established.

Exhibit A – ProTracts Application Controls Matrix

Exhibit A – Page 2 of 2

Master files and exception reporting help ensure all data processed are authorized.	• Since ProTracts is a web system, input to the system is real time. • ProTracts sends information to other systems.	• ITC has indicated that ProTracts processing to the financial system has master files and exception reporting.
All authorized transactions (data) are entered into and processed by the computer.	• Field staff must enter information into the system to complete applications, contracts, contract statuses, and payment requests.	• Performance issues with the system are causing the field staff to have problems getting information entered into the system.
Reconciliations are performed to verify data completeness.	• Field staff must enter information into the system to complete applications, contracts, contract status, and payment requests. • ProTracts sends information to other systems.	• Field staff must verify that they have entered the applicable information related to their applications, contracts, and payment requests. • Manual reconciliations are not being performed between ProTracts and the financial system.
Data entry design features contribute to data accuracy.	• NRCS did not have a specification detailing payment calculations. • ProTracts and Fund Manager screens were user-friendly.	• Payment calculations may not be accurate. However, without a payment specification, NRCS cannot determine if payments are accurately calculated.
Data validation and editing are performed to identify erroneous data.	• ProTracts data fields programmed to accept certain values.	• Based on field staff input, we determined that units were being incorrectly entered to derive a manual payment amount.
Erroneous data are captured, reported, investigated, and corrected.	• ProTracts has been programmed with a variety of business rules, which are intended to catch errors before they are entered. • NRCS relies on field and State office staff to review, identify, and correct errors in their data.	• NRCS did not have a review process in place for reviewing and authorizing information entered into ProTracts.
Review of output reports helps maintain data accuracy and validity.	• Field staff, State office staff, and national staff review various reports.	• NRCS did not have a review process in place for reviewing and authorizing information entered into ProTracts.

Exhibit B – *Agency Response*



United States Department of Agriculture

NRCS
Natural Resources Conservation Service
P.O. Box 2890
Washington, D.C. 20013

JUN 2 0 2006

SUBJECT: OIG Audit Report No. 10501-5-FM, Application
Controls – Program Contracts System (ProTracts)

TO: Robert W. Young
Assistant Inspector General for Audit
United States Department of Agriculture
Office of the Inspector General
Washington D.C. 20250

This memorandum transmits the Natural Responses Conservation Service's (NRCS) response to the Office of the Inspector General's (OIG) draft report, OIG 10501-5-FM Natural Resources Conservation Service Application Controls – Program Contracts System (ProTracts). This report provides valuable information that will help NRCS improve management and internal controls over the input, processing, and output of ProTracts data.

Section 1. Management of ProTracts Needs to Be Strengthened

OIG Recommendation 1.

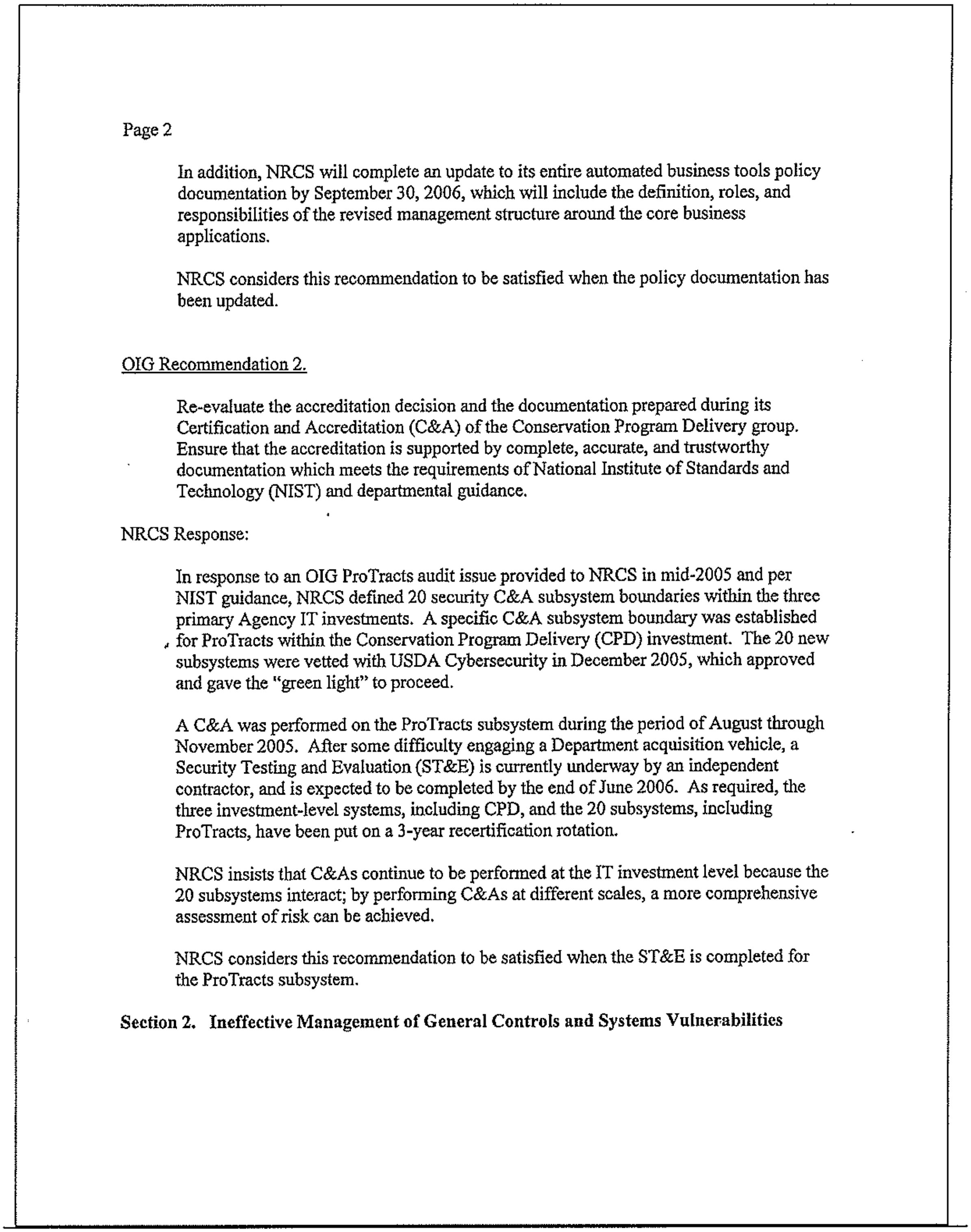
> NRCS should assign program managers as system and information owners for its business-critical applications and establish definite roles and responsibilities between the program managers and the technical group.

NRCS Response:

> In response to an OIG ProTracts audit issue provided to NRCS in mid-2005, NRCS formed and staffed an Agency field business tools team within the Programs Deputy area to provide business ownership and direct guidance to the core Agency program delivery applications, including ProTracts, and associated support applications. The Deputy Chief for Programs was assigned ownership for the ProTracts system. Two program business experts also were assigned to the Fort Collins, Colorado location to provide day-to-day guidance to the Information Technology Center (ITC) responsible for maintaining and enhancing the core applications. This has enabled the ITC to focus on its information technology (IT) technical responsibilities.

The Natural Resources Conservation Service provides leadership in a partnership effort to help people conserve, maintain, and improve our natural resources and environment.

An Equal Opportunity Provider and Employer



Page 2

In addition, NRCS will complete an update to its entire automated business tools policy documentation by September 30, 2006, which will include the definition, roles, and responsibilities of the revised management structure around the core business applications.

NRCS considers this recommendation to be satisfied when the policy documentation has been updated.

OIG Recommendation 2.

Re-evaluate the accreditation decision and the documentation prepared during its Certification and Accreditation (C&A) of the Conservation Program Delivery group. Ensure that the accreditation is supported by complete, accurate, and trustworthy documentation which meets the requirements of National Institute of Standards and Technology (NIST) and departmental guidance.

NRCS Response:

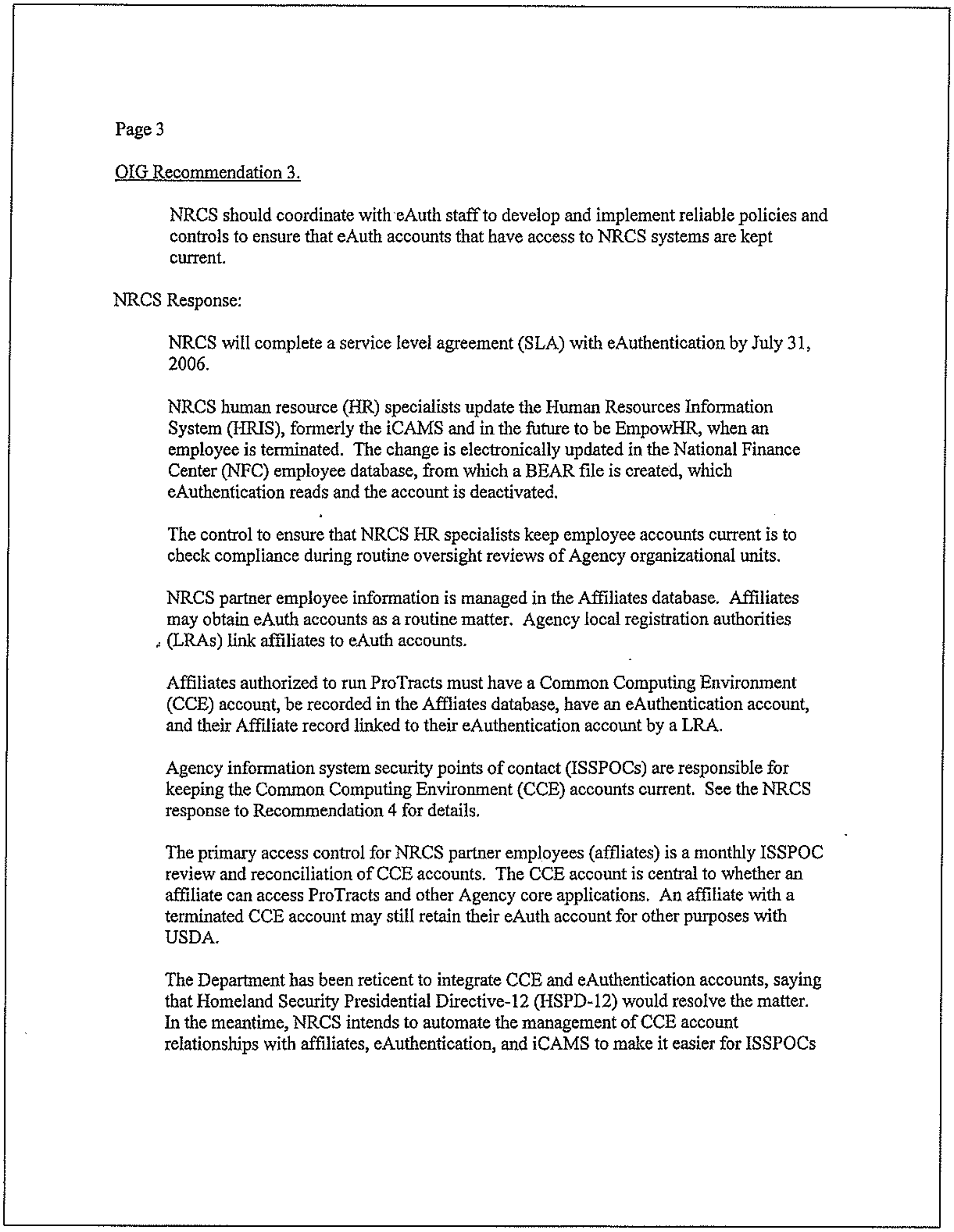
In response to an OIG ProTracts audit issue provided to NRCS in mid-2005 and per NIST guidance, NRCS defined 20 security C&A subsystem boundaries within the three primary Agency IT investments. A specific C&A subsystem boundary was established for ProTracts within the Conservation Program Delivery (CPD) investment. The 20 new subsystems were vetted with USDA Cybersecurity in December 2005, which approved and gave the "green light" to proceed.

A C&A was performed on the ProTracts subsystem during the period of August through November 2005. After some difficulty engaging a Department acquisition vehicle, a Security Testing and Evaluation (ST&E) is currently underway by an independent contractor, and is expected to be completed by the end of June 2006. As required, the three investment-level systems, including CPD, and the 20 subsystems, including ProTracts, have been put on a 3-year recertification rotation.

NRCS insists that C&As continue to be performed at the IT investment level because the 20 subsystems interact; by performing C&As at different scales, a more comprehensive assessment of risk can be achieved.

NRCS considers this recommendation to be satisfied when the ST&E is completed for the ProTracts subsystem.

Section 2. Ineffective Management of General Controls and Systems Vulnerabilities



OIG Recommendation 3.

> NRCS should coordinate with eAuth staff to develop and implement reliable policies and controls to ensure that eAuth accounts that have access to NRCS systems are kept current.

NRCS Response:

NRCS will complete a service level agreement (SLA) with eAuthentication by July 31, 2006.

NRCS human resource (HR) specialists update the Human Resources Information System (HRIS), formerly the iCAMS and in the future to be EmpowHR, when an employee is terminated. The change is electronically updated in the National Finance Center (NFC) employee database, from which a BEAR file is created, which eAuthentication reads and the account is deactivated.

The control to ensure that NRCS HR specialists keep employee accounts current is to check compliance during routine oversight reviews of Agency organizational units.

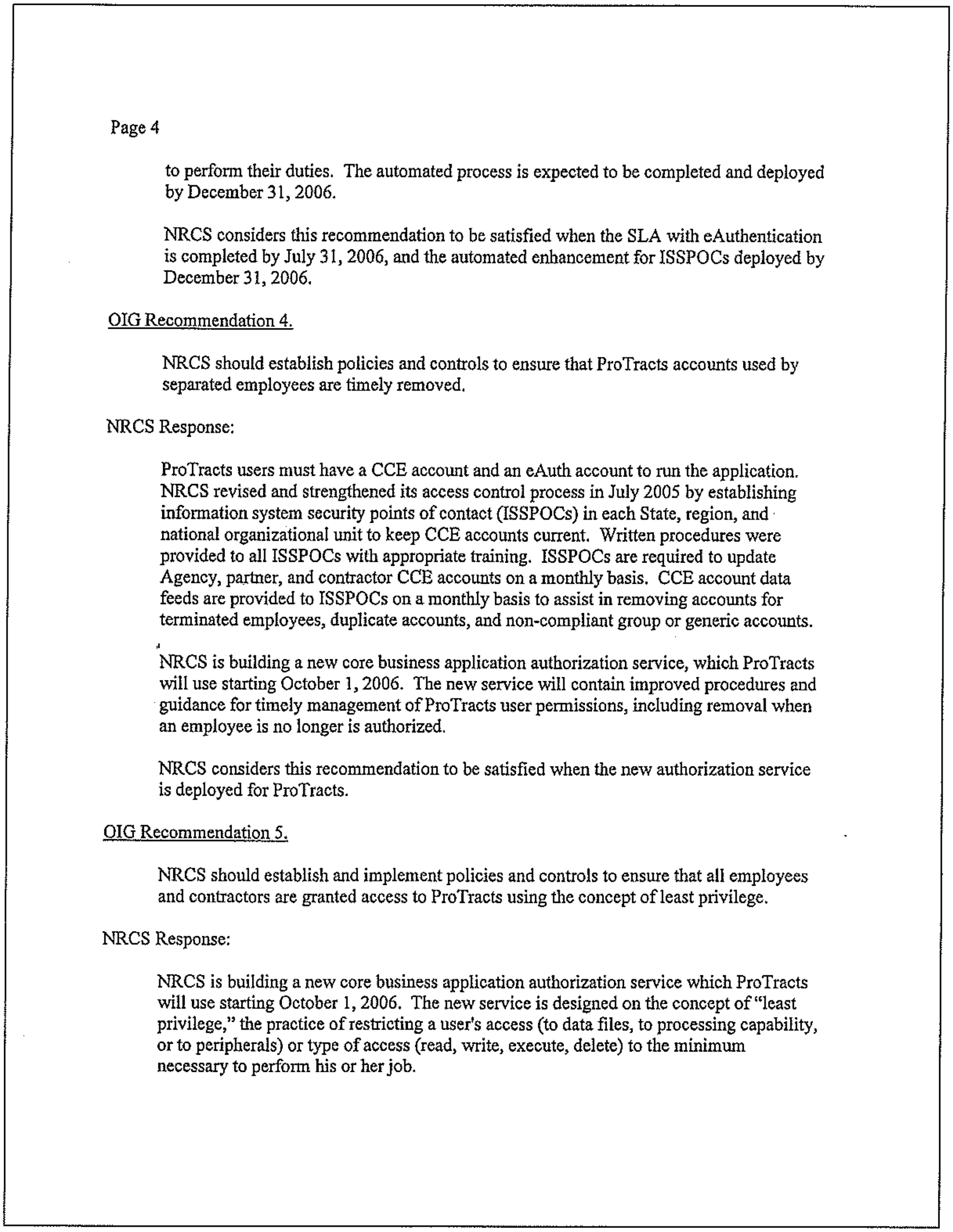
NRCS partner employee information is managed in the Affiliates database. Affiliates may obtain eAuth accounts as a routine matter. Agency local registration authorities (LRAs) link affiliates to eAuth accounts.

Affiliates authorized to run ProTracts must have a Common Computing Environment (CCE) account, be recorded in the Affliates database, have an eAuthentication account, and their Affiliate record linked to their eAuthentication account by a LRA.

Agency information system security points of contact (ISSPOCs) are responsible for keeping the Common Computing Environment (CCE) accounts current. See the NRCS response to Recommendation 4 for details.

The primary access control for NRCS partner employees (affliates) is a monthly ISSPOC review and reconciliation of CCE accounts. The CCE account is central to whether an affiliate can access ProTracts and other Agency core applications. An affiliate with a terminated CCE account may still retain their eAuth account for other purposes with USDA.

The Department has been reticent to integrate CCE and eAuthentication accounts, saying that Homeland Security Presidential Directive-12 (HSPD-12) would resolve the matter. In the meantime, NRCS intends to automate the management of CCE account relationships with affiliates, eAuthentication, and iCAMS to make it easier for ISSPOCs



to perform their duties. The automated process is expected to be completed and deployed by December 31, 2006.

NRCS considers this recommendation to be satisfied when the SLA with eAuthentication is completed by July 31, 2006, and the automated enhancement for ISSPOCs deployed by December 31, 2006.

OIG Recommendation 4.

NRCS should establish policies and controls to ensure that ProTracts accounts used by separated employees are timely removed.

NRCS Response:

ProTracts users must have a CCE account and an eAuth account to run the application. NRCS revised and strengthened its access control process in July 2005 by establishing information system security points of contact (ISSPOCs) in each State, region, and national organizational unit to keep CCE accounts current. Written procedures were provided to all ISSPOCs with appropriate training. ISSPOCs are required to update Agency, partner, and contractor CCE accounts on a monthly basis. CCE account data feeds are provided to ISSPOCs on a monthly basis to assist in removing accounts for terminated employees, duplicate accounts, and non-compliant group or generic accounts.

NRCS is building a new core business application authorization service, which ProTracts will use starting October 1, 2006. The new service will contain improved procedures and guidance for timely management of ProTracts user permissions, including removal when an employee is no longer is authorized.

NRCS considers this recommendation to be satisfied when the new authorization service is deployed for ProTracts.

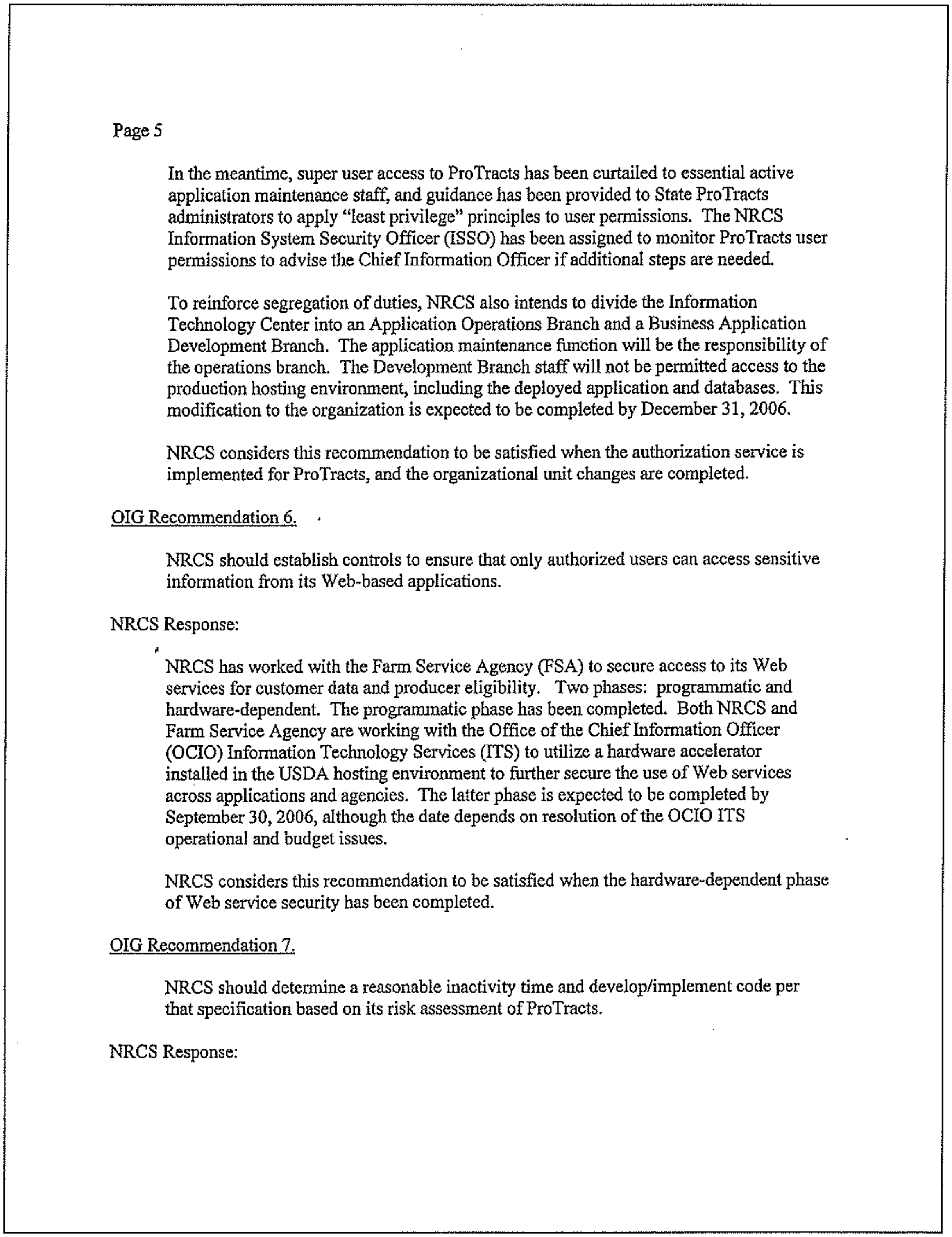
OIG Recommendation 5.

NRCS should establish and implement policies and controls to ensure that all employees and contractors are granted access to ProTracts using the concept of least privilege.

NRCS Response:

NRCS is building a new core business application authorization service which ProTracts will use starting October 1, 2006. The new service is designed on the concept of "least privilege," the practice of restricting a user's access (to data files, to processing capability, or to peripherals) or type of access (read, write, execute, delete) to the minimum necessary to perform his or her job.

Exhibit B – Agency Response



In the meantime, super user access to ProTracts has been curtailed to essential active application maintenance staff, and guidance has been provided to State ProTracts administrators to apply "least privilege" principles to user permissions. The NRCS Information System Security Officer (ISSO) has been assigned to monitor ProTracts user permissions to advise the Chief Information Officer if additional steps are needed.

To reinforce segregation of duties, NRCS also intends to divide the Information Technology Center into an Application Operations Branch and a Business Application Development Branch. The application maintenance function will be the responsibility of the operations branch. The Development Branch staff will not be permitted access to the production hosting environment, including the deployed application and databases. This modification to the organization is expected to be completed by December 31, 2006.

NRCS considers this recommendation to be satisfied when the authorization service is implemented for ProTracts, and the organizational unit changes are completed.

OIG Recommendation 6.

NRCS should establish controls to ensure that only authorized users can access sensitive information from its Web-based applications.

NRCS Response:

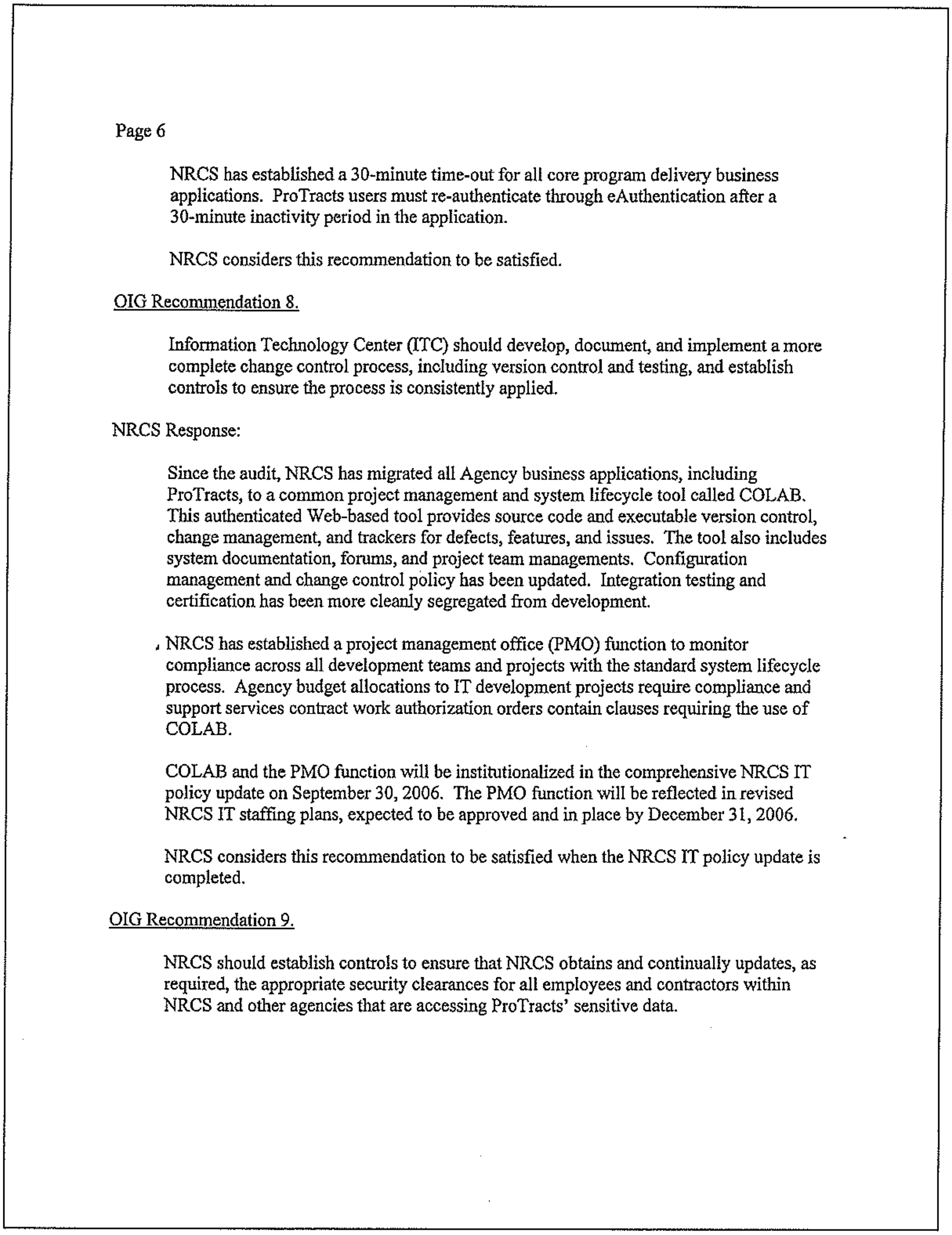
NRCS has worked with the Farm Service Agency (FSA) to secure access to its Web services for customer data and producer eligibility. Two phases: programmatic and hardware-dependent. The programmatic phase has been completed. Both NRCS and Farm Service Agency are working with the Office of the Chief Information Officer (OCIO) Information Technology Services (ITS) to utilize a hardware accelerator installed in the USDA hosting environment to further secure the use of Web services across applications and agencies. The latter phase is expected to be completed by September 30, 2006, although the date depends on resolution of the OCIO ITS operational and budget issues.

NRCS considers this recommendation to be satisfied when the hardware-dependent phase of Web service security has been completed.

OIG Recommendation 7.

NRCS should determine a reasonable inactivity time and develop/implement code per that specification based on its risk assessment of ProTracts.

NRCS Response:



Page 6

NRCS has established a 30-minute time-out for all core program delivery business applications. ProTracts users must re-authenticate through eAuthentication after a 30-minute inactivity period in the application.

NRCS considers this recommendation to be satisfied.

<u>OIG Recommendation 8.</u>

Information Technology Center (ITC) should develop, document, and implement a more complete change control process, including version control and testing, and establish controls to ensure the process is consistently applied.

NRCS Response:

Since the audit, NRCS has migrated all Agency business applications, including ProTracts, to a common project management and system lifecycle tool called COLAB. This authenticated Web-based tool provides source code and executable version control, change management, and trackers for defects, features, and issues. The tool also includes system documentation, forums, and project team managements. Configuration management and change control policy has been updated. Integration testing and certification has been more cleanly segregated from development.

NRCS has established a project management office (PMO) function to monitor compliance across all development teams and projects with the standard system lifecycle process. Agency budget allocations to IT development projects require compliance and support services contract work authorization orders contain clauses requiring the use of COLAB.

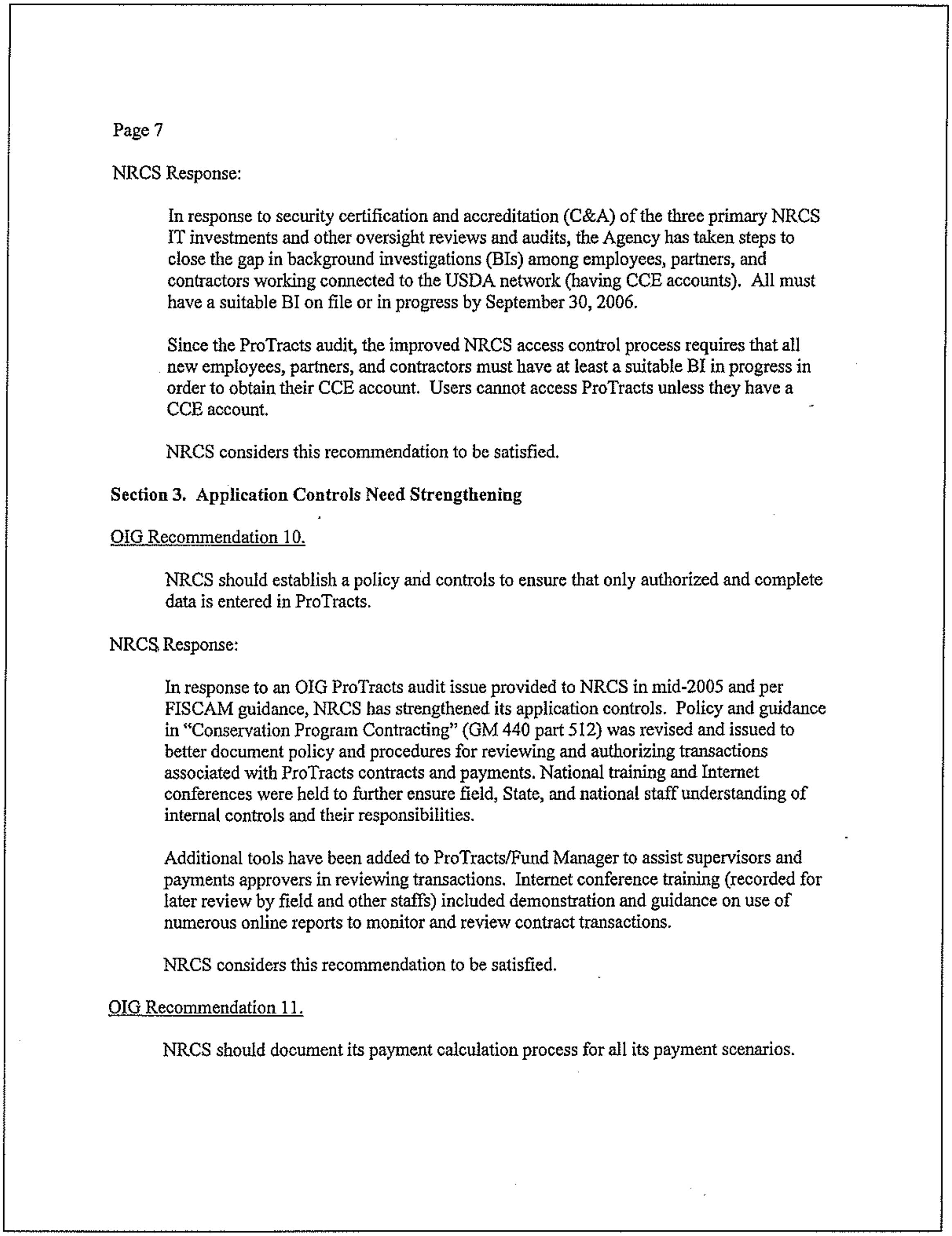
COLAB and the PMO function will be institutionalized in the comprehensive NRCS IT policy update on September 30, 2006. The PMO function will be reflected in revised NRCS IT staffing plans, expected to be approved and in place by December 31, 2006.

NRCS considers this recommendation to be satisfied when the NRCS IT policy update is completed.

<u>OIG Recommendation 9.</u>

NRCS should establish controls to ensure that NRCS obtains and continually updates, as required, the appropriate security clearances for all employees and contractors within NRCS and other agencies that are accessing ProTracts' sensitive data.

Exhibit B – Agency Response



NRCS Response:

In response to security certification and accreditation (C&A) of the three primary NRCS IT investments and other oversight reviews and audits, the Agency has taken steps to close the gap in background investigations (BIs) among employees, partners, and contractors working connected to the USDA network (having CCE accounts). All must have a suitable BI on file or in progress by September 30, 2006.

Since the ProTracts audit, the improved NRCS access control process requires that all new employees, partners, and contractors must have at least a suitable BI in progress in order to obtain their CCE account. Users cannot access ProTracts unless they have a CCE account.

NRCS considers this recommendation to be satisfied.

Section 3. Application Controls Need Strengthening

OIG Recommendation 10.

NRCS should establish a policy and controls to ensure that only authorized and complete data is entered in ProTracts.

NRCS Response:

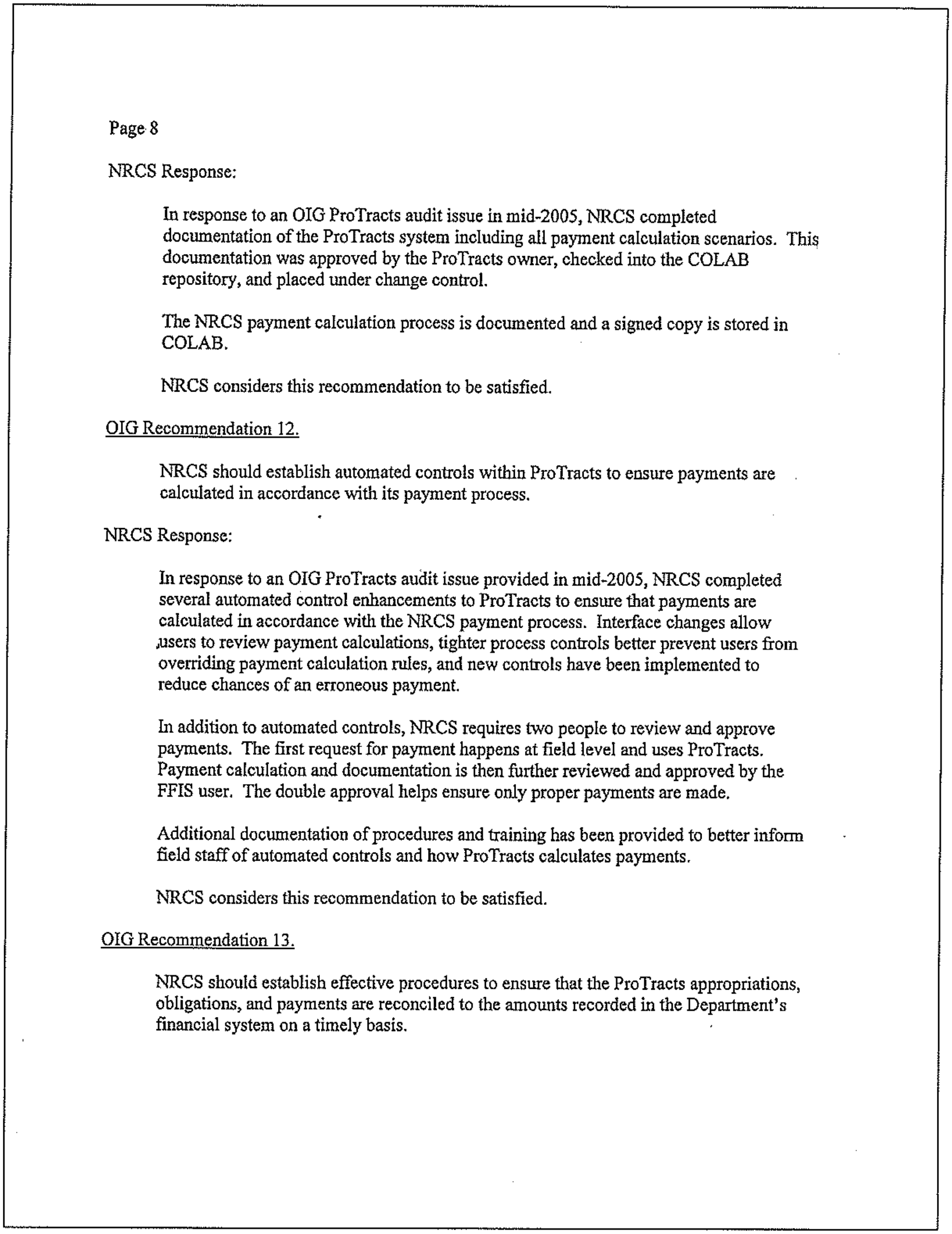
In response to an OIG ProTracts audit issue provided to NRCS in mid-2005 and per FISCAM guidance, NRCS has strengthened its application controls. Policy and guidance in "Conservation Program Contracting" (GM 440 part 512) was revised and issued to better document policy and procedures for reviewing and authorizing transactions associated with ProTracts contracts and payments. National training and Internet conferences were held to further ensure field, State, and national staff understanding of internal controls and their responsibilities.

Additional tools have been added to ProTracts/Fund Manager to assist supervisors and payments approvers in reviewing transactions. Internet conference training (recorded for later review by field and other staffs) included demonstration and guidance on use of numerous online reports to monitor and review contract transactions.

NRCS considers this recommendation to be satisfied.

OIG Recommendation 11.

NRCS should document its payment calculation process for all its payment scenarios.



NRCS Response:

In response to an OIG ProTracts audit issue in mid-2005, NRCS completed documentation of the ProTracts system including all payment calculation scenarios. This documentation was approved by the ProTracts owner, checked into the COLAB repository, and placed under change control.

The NRCS payment calculation process is documented and a signed copy is stored in COLAB.

NRCS considers this recommendation to be satisfied.

OIG Recommendation 12.

NRCS should establish automated controls within ProTracts to ensure payments are calculated in accordance with its payment process.

NRCS Response:

In response to an OIG ProTracts audit issue provided in mid-2005, NRCS completed several automated control enhancements to ProTracts to ensure that payments are calculated in accordance with the NRCS payment process. Interface changes allow users to review payment calculations, tighter process controls better prevent users from overriding payment calculation rules, and new controls have been implemented to reduce chances of an erroneous payment.

In addition to automated controls, NRCS requires two people to review and approve payments. The first request for payment happens at field level and uses ProTracts. Payment calculation and documentation is then further reviewed and approved by the FFIS user. The double approval helps ensure only proper payments are made.

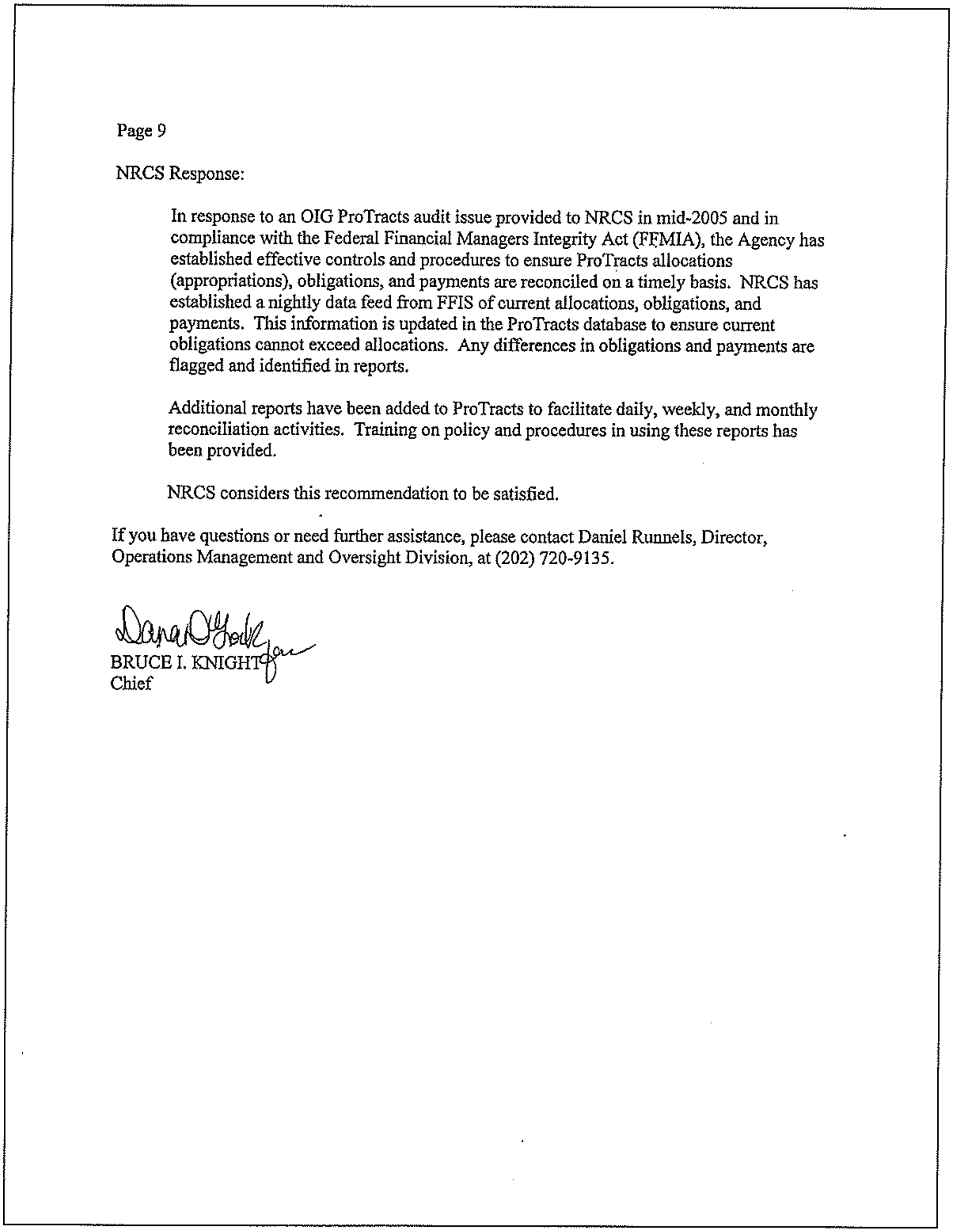
Additional documentation of procedures and training has been provided to better inform field staff of automated controls and how ProTracts calculates payments.

NRCS considers this recommendation to be satisfied.

OIG Recommendation 13.

NRCS should establish effective procedures to ensure that the ProTracts appropriations, obligations, and payments are reconciled to the amounts recorded in the Department's financial system on a timely basis.

Exhibit B – Agency Response



Page 9

NRCS Response:

In response to an OIG ProTracts audit issue provided to NRCS in mid-2005 and in compliance with the Federal Financial Managers Integrity Act (FFMIA), the Agency has established effective controls and procedures to ensure ProTracts allocations (appropriations), obligations, and payments are reconciled on a timely basis. NRCS has established a nightly data feed from FFIS of current allocations, obligations, and payments. This information is updated in the ProTracts database to ensure current obligations cannot exceed allocations. Any differences in obligations and payments are flagged and identified in reports.

Additional reports have been added to ProTracts to facilitate daily, weekly, and monthly reconciliation activities. Training on policy and procedures in using these reports has been provided.

NRCS considers this recommendation to be satisfied.

If you have questions or need further assistance, please contact Daniel Runnels, Director, Operations Management and Oversight Division, at (202) 720-9135.

Dana D York for

BRUCE I. KNIGHT
Chief